ÖN BİLGİ

Bu belgenin resmi adresi bulunamamıştır. Alternatif adreste yedeklenmiştir. Bu belge

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Web%20Uygulama%20G%C3%BCnl%C3%BC%C4%9F%C3%BCne%20Kartal%20Bak%C4%B1%C5%9F%C4%B1.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Eger güvenlik testlerinde Metasploit kullanıyorsanız W3af'yi de web uygulamaları için yazılmıs Metasploit olarak kabul edebilirsiniz.

(Page 2)

2)

W3af Nasıl Çalısır?
Güvenlik testlerinin temel prensibi olan Kesfet -> *Kontrol Et/Denetle* -> *Saldır* metodu W3af için de geçerli. Bünyesinde bulunan eklentiler sayesinde öncelikle test edilen sistemde zayıflık içerebilecek hedefler (url, form vs) bulunur. Sonra bulunan bu hedeflere özel veriler gönderilerek zayıflıklar tespit edilir ve bu zayıflık noktaları exploit edilmeye çalısılır. Exploitin türüne göre sistemde shell açılabilir ya da ilgili zayıflıga ait veriler sistemden alınır.

(page 2)